CLAIMS

1. An information storage medium storing:

an encrypted content;

encryption key information needed in a process of decoding the encrypted content;

an information storage medium ID which is an identifier uniquely assigned to the information storage medium; and

an information storage medium ID revocation list which is a list of information storage medium IDs determined as fraudulent.

2. An information storage medium according to Claim 1, wherein the information storage medium ID revocation list includes a tampering check value for checking whether data described in the information storage medium ID revocation list is untamperred.

3. An information storage medium according to Claim 1, wherein the encryption key information includes an enabling key block (EKB) as encryption key data from which a key used to decrypt the encrypted content is extractable.

4. An information storage medium according to Claim 3, wherein the enabling key block (EKB) is encryption key

information that can be decrypted based on a device node key (DNK) provided in the form of a hierarchical key-distribution tree structure to an information processing apparatus that is a device using the information storage medium.

5. An information processing apparatus for playing back a content stored on an information storage medium, comprising:

a memory in which an information storage medium ID revocation list, which is a list of information storage medium IDs determined as fraudulent, is stored,

wherein a check is made as to whether an information storage medium ID stored on the information storage medium is identical to one of revoked information storage medium IDs described in the storage medium information ID revocation list stored in the memory, and, if the information storage medium ID stored on the information storage medium is not identical to any one of the revoked information storage medium IDs described in the information storage medium ID revocation list, a content playback process is performed.

6. An information processing apparatus according to Claim 5, wherein a tampering check process is performed to

check whether no tampering is made on the information storage medium ID revocation list stored on the information storage medium, and, if the check indicates that no tampering is made, the version of the information storage medium ID revocation list stored on the information storage medium is compared with the version of that stored in the memory, and the information storage medium ID revocation list stored in the memory is updated by storing the information storage medium ID revocation list stored on the information storage medium into the memory when the version of the information storage medium ID revocation list is newer than the version of that stored in the memory.

7. An information processing apparatus according to Claim 5, wherein:

the information processing apparatus has a device node key (DNK) as key information provided in the form of a hierarchical key-distribution tree structure; and

a key used to decrypt an encrypted content stored on the information storage medium is extracted by decoding, based on the device node key (DNK), an enabling key block (EKB) stored as encryption key information on the information storage medium.

8. An information storage medium production apparatus

that produces an information storage medium such that:

information is stored on the information storage medium, the information including

an encrypted content,

encryption key information needed in a process of decoding the encrypted content, and

an information storage medium ID revocation list which is a list of information storage medium IDs determined as fraudulent, and

an information storage medium ID, which is an identifier uniquely assigned to each information storage medium, is stored on each produced information storage medium such that each information storage medium has a different information storage medium ID.

9. An information storage medium production apparatus according to Claim 8, wherein the information storage medium ID revocation list includes a tampering check value for checking whether data described in the information storage medium ID revocation list is untamperred.

10. An information storage medium production apparatus according to Claim 8, wherein the encryption key information includes an enabling key block (EKB) as encryption key data to be applied in the decryption of the encrypted content.

11. An information processing method of playing back a content stored on an information storage medium, comprising the steps of:

reading information storage medium ID stored on the information storage medium;

checking whether the information storage medium ID stored on the information storage medium is identical to one of revoked information storage medium IDs described in a storage medium information ID revocation list, which is a list of invalid information storage medium IDs and which is stored in a memory of an information processing apparatus; and

playing back the content if and only if the information storage medium ID stored on the information storage medium is not identical to any one of the revoked information storage medium IDs described in the information storage medium ID revocation list.

12. An information processing method according to Claim 11, further comprising the step of updating the list, the list updating step including the sub-steps of performing a tampering check process to check whether no tampering is made on the information storage medium ID revocation list stored on the information storage medium, if the check

indicates that no tampering is made, comparing the version of the information storage medium ID revocation list stored on the information storage medium with the version of that stored in the memory, and updating the information storage medium ID revocation list stored in the memory by storing the information storage medium ID revocation list stored on the information storage medium into the memory when the version of the information storage medium ID revocation list is newer than the version of that stored in the memory.

13. An information processing method according to Claim 11, further comprising the step of acquiring a key used to decode an encrypted content stored on the information storage medium by decoding an enabling key block (EKB) stored as encryption key information on the information storage medium, the decoding of the enabling key block (EKB) being based on a device node key (DNK) provided as key information provided in the form of a hierarchical key-distribution tree structure.

14. A method of producing an information storage medium, comprising the step of:

storing, on the information storage medium, an encrypted content, encryption key information needed in a process of decoding the encrypted content, and an

information storage medium ID revocation list which is a list of information storage medium IDs determined as fraudulent; and

storing an information storage medium ID, which is an identifier uniquely assigned to each information storage medium, on each produced information storage medium such that each information storage medium has a different information storage medium ID.

15. A computer program that executes a process of playing back a content stored on an information storage medium, the process comprising the steps of:

reading information storage medium ID stored on the information storage medium;

checking whether the information storage medium ID stored on the information storage medium is identical to one of revoked information storage medium IDs described in a storage medium information ID revocation list, which is a list of invalid information storage medium IDs and which is stored in a memory of an information processing apparatus; and

playing back the content if and only if the information storage medium ID stored on the information storage medium is not identical to any one of the revoked information storage medium IDs described in the information storage

medium ID revocation list.